UNIVERSIDAD DE COSTA RICA
SISTEMA DE ESTUDIOS DE POSGRADO

AUDITORÍA PARA EVALUAR EL GOBIERNO DE LAS TECNOLOGÍAS DE INFORMACIÓN EN UNA ASOCIACIÓN PRIVADA SIN FINES DE LUCRO, CUYOS PRODUCTOS APOYAN AL SECTOR EDUCATIVO COSTARRICENSE

Trabajo final de graduación sometido a la consideración de la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas para optar al grado y título de **Maestría Profesional en Auditoría de Tecnologías de Información**

SUSTENTANTE:

Carmen Murillo Murillo

Ciudad Universitaria Rodrigo Facio, Costa Rica
2018

DEDICATORIA

Este proyecto está dedicado a Dios, por brindarme la salud y bendecirme con las oportunidades que han permitido cumplir mis objetivos.

A mi esposo, por su apoyo y comprensión incondicional en todos mis proyectos de vida.

A mis padres, quienes me dieron las herramientas que me ha permitido llegar acá y me mostraron el camino de la superación

A mi hermano, Mainor, por estar en todo momento dispuesto a ayudarme y ser un compañero de vida

A mis compañeros, quienes se convirtieron en la principal fuente de aprendizaje en este recorrido.

AGRADECIMIENTOS

Agradezco al equipo de la Asociación, primero que todo por realizar una labor que constituye un pilar fundamental en la sociedad costarricense y en segundo lugar por abrirme las puertas para realizar este proyecto, un especial agradecimiento a su Gerente, quien siempre estuvo dispuesta a ayudarme y dedicarme parte de su valioso tiempo.

A mi tutor, Marco V. Gámez Acuña por su consejo y guía, sus aportes constituyen parte importante de este proyecto.

Al coordinador, Gino Ramírez Solís, su constancia en el seguimiento y su consejo fue clave para la culminación de este proyecto.

"Este trabajo final de investigación aplicada fue aceptado por la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas de la Universidad de Costa Rica, como requisito parcial para optar al grado y título de Maestría Profesional en Auditoría de Tecnologías de Información"

_____

MSc. Gino Ramírez Solís

Profesor Guía

_____

MSc. Marco V. Gámez Acuña

Tutor

_____

MSc. Hanie Cordero Calderón

Lectora de Empresa

_____

MSc. Ridiguer Artavia Barboza

Director Programa en Posgrado en Administración y Dirección de Empresas

_____

Carmen Murillo Murillo

Sustentante

TABLA DE CONTENIDOS

RESUMEN

El objetivo del presente trabajo es realizar una evaluación del gobierno de las tecnologías de información (TI) de una asociación sin fines de lucro, con el propósito de mejorar el sistema de control interno y la alineación estratégica de las tecnologías de información con los objetivos del negocio.

El proyecto desarrollado tuvo como alcance aplicar una auditoría que permitiera evaluar el gobierno de las TI, para ello se desarrolló un programa de trabajo, el cual se basó en el programa sugerido por ISACA para el proceso “EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno”.

Como parte de la ejecución del programa de auditoría se desarrollaron diferentes plantillas, que permitieron recopilar la evidencia requerida para sustentar los hallazgos, conclusiones y recomendaciones.

El estudio aplicado permitió identificar que la organización no ha diseñado ni mantiene funcionando estructuras de gobierno de las tecnologías de información, por lo que se presenta una brecha significativa con las mejores prácticas. Esto debido principalmente a la carencia de los siguientes factores: principios relacionados con el gobierno de las TI, una evaluación de la alineación de las TI con la estrategia de la Asociación, un plan estratégico de TI, definición formal de los roles de las estructuras organizativas en relación con este proceso, capacitación y concientización de los órganos de dirección y gerencia en relación con temas de gobierno de las TI y de marcos y políticas formales de gobernanza de TI.

Para la implementación de las mejoras necesarias, en el presente informe, se proponen recomendaciones que incorporan a los órganos de dirección y a la Gerencia de Operaciones, así mismo se sugiere la creación de un Comité de TI y además el uso de expertos externos que contribuyan a robustecer el proceso.

ABSTRACT

The main objective of this project is to perform an assessment of the government of Information Technology (IT) of a non-profit association to improve the internal control system and the strategic alignment of information technologies with business objectives.

The project developed had the scope of applying an audit that would allow the evaluation of IT government, a work program was developed for this purpose and was based on the program suggested by ISACA for the process "EDM01 Ensure Governance Framework Setting and Maintenance Audit/Assurance Program".

As part of the execution of the audit program, different templates were developed which allowed to compile the required evidence to support the findings, conclusions and recommendations.

The analysis done allowed to identify that the organization has not designed nor maintains performing governance structures of information technologies, so there is a significant gap with best practices. This is mainly due to the lack of the following factors: principles related to the government of IT, an assessment of the IT alignment with the Association strategy, a strategic IT plan, formal roles definition for organizational structures in relation to this process, training and awareness of the management in relation to IT government issues and formal IT government frameworks and policies.

For the implementation of the necessary improvements, this report proposes recommendations that incorporate the different management departments and Operations Management, and suggests the creation of an IT Committee and also the use of external experts to contributte strengthen the process.

NOMENCLATURA

Siglas	Definición
TI	Tecnologías de Información
PYMES	Pequeñas y medianas empresas
OCDE	Organización para la Cooperación y el Desarrollo Económicos
CGR	Contraloría General de la República
CONASSIF	Consejo Nacional de Supervisión del Sistema Financiero
ISACA	Asociación de Auditoría y Control de Sistemas de Información

CAPÍTULO 1- INTRODUCCIÓN

1.1 Objetivos

1.1.1 Objetivo General

Realizar una evaluación del gobierno de las tecnologías de información (TI) de una asociación sin fines de lucro, con el propósito de mejorar el sistema de control interno y la alineación estratégica de las tecnologías y el negocio.

1.1.2 Objetivos específicos

a. Determinar la suficiencia de las actividades realizadas por la Asociación relacionadas con las tecnologías de información y los aspectos claves en el aporte de valor y optimización de la función de TI.
b. Determinar la suficiencia del control interno del proceso evaluado, sus acciones en pro de la gobernabilidad de las TI y emitir recomendaciones de los aspectos sujetos a mejora encontrados.
c. Diseñar herramientas y papeles de trabajo para sustentar el proceso de auditoría de este proyecto, a partir de los conocimientos adquiridos en la maestría.

1.2 Alcance

El proyecto en desarrollo tiene como alcance aplicar una auditoría que permita evaluar el gobierno de las tecnologías de información en una asociación privada sin fines de lucro; lo cual implica valorar cómo la organización analiza y articula los requerimientos de tecnologías de la información; así como las acciones para la puesta en marcha y mantenimiento de sus estructuras, procesos y prácticas de la gestión que soportan las TI para alcanzar la misión, las metas y objetivos de la empresa.

Se considera en su alcance temporal, como una investigación transversal o sincrónica, ya que se realiza en un momento dado (noviembre 2017 hasta abril 2018) y los datos o situaciones analizadas también pertenecen a un periodo dado (enero-diciembre de 2017).

El estudio se enfocará en valorar las actividades relacionadas con evaluar, orientar y supervisar el sistema de gobierno de las TI de la Asociación basado en el proceso de COBIT 5 “EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno”, de forma que le permita a la Asociación obtener una referencia para generar oportunidades y ventajas competitivas mediante el uso efectivo de las TI desde un adecuado gobierno.

1.3 Justificación

Este trabajo final de graduación tiene como fin beneficiar a una asociación privada sin fines de lucro, cuyo giro de negocio se basa en ofrecer al sector educativo costarricense materiales didácticos y herramientas educativas para los estudiantes y docentes, por lo que indirectamente también se está beneficiando a dicha población.

El beneficiar con un trabajo de graduación al sector educativo costarricense y una asociación sin fines de lucro, genera un aporte a la misión del Sistema de Estudios de Posgrado, que busca la formación de profesionales con visión humanista y responsabilidad social, mediante la aplicación de los conocimientos de la maestría.

Adicionalmente, diseñando un proceso de auditoría de gobierno para una empresa de tales características podrá servir de base para futuras aplicaciones en pequeñas y medianas empresas (PYMES) del mercado costarricense; lo cual les permitiría auditar su gestión de las TI desde su gobierno y potenciar su negocio identificando oportunidades de mejora y mostrando cómo, a pesar de su tamaño, la gobernanza de las TI se vuelve un pilar fundamental para su crecimiento.

1.4 Marco metodológico

1.4.1 Clasificación de la investigación

El presente trabajo, según Barrantes Echeverría (1999), se clasifica como una investigación aplicada, pues se aplica el conocimiento adquirido durante la maestría a un caso real en una asociación privada costarricense, con la finalidad de detectar aspectos sujetos a mejora en el control interno del lugar donde se aplica. El estudio realizado no pretende aportar un conocimiento teórico nuevo al campo de la auditoría, sino atacar potenciales problemas generadores de riesgo en el tema evaluado, que en este caso es el gobierno de las tecnologías de información en una asociación privada.

La investigación se considera transversal o sincrónica, al realizarse en un momento dado, con datos y situaciones analizadas en el periodo establecido en el alcance de este proyecto, teniendo de esta forma, un alcance temporal.

Según su profundidad u objeto, se puede catalogar como descriptiva, ya que describe una condición encontrada, que se valora contra unos criterios normativos establecidos que rigen el tema evaluado tanto a nivel interno como externo (ámbito costarricense) y se emiten aspecto de mejora, si así se determina.

Respecto a su enfoque o medición, se considera cualitativa, ya que se describirán situaciones ordinarias de la institución evaluada sin cuantificar o manipular datos numéricos específicos, más que los que se observan o responden en instrumentos cualitativos. Tiene lugar en el campo y no en un laboratorio, con situaciones naturales y libertad de acción de los observados.

La validez de la investigación radica en la evidencia que recaba el sustentante durante su trabajo de campo y en la realización del debido proceso de ejecución. La confiabilidad se ampara en el diseño de los instrumentos denominados como “Papeles de Trabajo” que se basan en la normativa (interna y externa), estándares, criterio experto y mejores prácticas en el campo evaluado.

1.4.2 Detalle de metodología e instrumentos a utilizar

Para iniciar con el marco metodológico se considera pertinente definir los siguientes dos conceptos:

Método: manera de ordenar una actividad, orden sistemático que se impone en la investigación, camino para llegar a cierto resultado, que se compone de varias técnicas. (Barrantes Echeverría, 1999)

Técnica: es un conjunto de instrumentos de medición, elaborados con base en los conocimientos, mismos que pueden ser de medición o de recolección de la información. (Barrantes Echeverría, 1999)

Considerando que la asociación donde se realiza el trabajo pertenece al sector privado y que no posee una metodología para realizar auditorías, se tomará como norma base las “Normas generales de Auditoría para Sector Público” (CGR, 2014), que aun cuando son de acatamiento obligatorio únicamente para el sector público, se consideran una mejor práctica dentro del ámbito costarricense; se adaptarán las normas 203, 204, 205 y 207 de este marco como método para el presente trabajo de la siguiente manera:

Norma 203. Planificación

La auditoría del gobierno de TI de la asociación privada se planificará de forma que garantice la realización de una labor de alta calidad de un modo económico, eficiente y eficaz y de manera oportuna (momento) y de acuerdo con los principios de la buena gestión de proyectos.

La planificación de la auditoría debe permitir un uso eficiente de los recursos involucrados y se puedan incorporar los ajustes que correspondan durante su desarrollo; para lo anterior, se debe tener claro el objetivo, naturaleza, alcance, oportunidad y plazo para llevar a cabo el trabajo en el tiempo establecido. Además, debe obtener un conocimiento de la entidad, la comprensión del sistema de control

interno relacionado con el asunto objeto de auditoría, así como la identificación de los criterios de auditoría que serán aplicados.

Con los insumos de información y conocimiento, se realizará una evaluación del riesgo, que conduzca a seleccionar las áreas a auditar en la actividad de examen y permitirá la elaboración del Programa de Auditoría.

En la planificación se debe preparar y aprobar el programa específico que el postulante elaboró, para ser ejecutado durante la actividad de examen.

Instrumentos diseñados en esta etapa

- **Cuestionarios.** Al personal encargado del gobierno de TI, a usuarios respecto a su percepción del gobierno de TI y cualquier otro personal de interés.
- **Plantillas de trabajo.** Papeles de trabajo para evaluar o describir condiciones encontradas, listas de chequeo, cuadros resúmenes de información recopilada, resultados de pruebas, hojas de recolección de hallazgos, etc.
- **Guías de entrevistas.** Al personal encargado del gobierno de TI, a los entes rectores de emitir y aprobar las políticas y procedimientos internos en esta materia, a usuarios respecto a su percepción del gobierno de TI y cualquier otro personal de interés.
- **Mapa o Cuadro de Riesgo.** Es una herramienta que tiene por objeto mostrar gráficamente el diagnóstico del proceso de evaluación de riesgos que se identificaron en esta etapa de Planificación. Se determina mediante la interacción de la probabilidad o frecuencia por el impacto de los tipos de riesgos en los diferentes procesos, actividades o funciones de un negocio.

- **Programa de trabajo.** Es un documento formal que se utiliza como guía metodológica en la realización del trabajo. El programa indica la descripción de actividades a desarrollar de acuerdo con un orden y una lógica, y dentro de un periodo o tiempo determinado.

Norma 204. Examen o trabajo de campo

Durante la actividad de examen se debe ejecutar el programa realizado en la etapa de planificación. Se ejecutan en forma ordenada las actividades dispuestas, lo cual conlleva a realizar pruebas, evaluar controles y recolectar la evidencia necesaria mediante la utilización de técnicas y prácticas de auditoría para determinar, justificar y presentar apropiadamente los hallazgos de auditoría, con sus atributos de criterio, condición, causa y efecto.

Se aplican todos los papeles de trabajo diseñados en la etapa de planificación y cualquier otro requerido de acuerdo con los hallazgos encontrados, todo siguiendo el debido proceso tanto de la ejecución como en la recolección de evidencia; se verifica la calidad y trazabilidad desde el programa de trabajo hasta el último papel de trabajo diseñado y aplicado.

Instrumentos aplicados en esta etapa

- **Cuestionarios.** Al personal encargado del gobierno de TI, a usuarios respecto a su percepción del gobierno de TI y cualquier otro personal de interés.
- **Plantillas de trabajo.** Papeles de trabajo para evaluar o describir condiciones encontradas, listas de chequeo, cuadros resúmenes de información recopilada, resultados de pruebas, etc.
- **Entrevistas.** Al personal encargado del gobierno de TI, a los entes rectores de emitir y aprobar las políticas y procedimientos internos en esta materia, a usuarios respecto a su percepción del gobierno de TI y cualquier otro personal de interés.
- **Programa de trabajo.** Es un documento formal que se utiliza como guía metodológica en la realización del trabajo. El programa indica la descripción de actividades a desarrollar de acuerdo con un orden y una lógica, y dentro de un periodo o tiempo determinado.

- **Hojas de hallazgos.** Se recolectan todas las averiguaciones en la hoja de hallazgos correspondiente.

Norma 207 Evidencia

Los hallazgos de auditoría contenidos en los informes están sustentados en evidencia suficiente, competente y pertinente, obtenida por los medios legales y técnicos aplicables.

Entregables en esta etapa

- **Diseño del Informe Borrador.** Se diseña el informe Borrador, para aprobación.

Norma 205. Comunicación de resultados

Una vez concluido el trabajo de campo y aprobado el Informe Borrador, se les comunica a las instancias correspondientes de la Asociación sobre los principales resultados, las conclusiones y las recomendaciones producto de la auditoría que se llevó a cabo, lo que constituirá la base para el mejoramiento de los asuntos examinados.

El informe preliminar de auditoría se elabora en un lenguaje sencillo, debe ser objetivo, conciso, claro, completo, exacto e imparcial, basado en hechos y respaldado con evidencia suficiente, competente y pertinente.

El postulante efectúa una conferencia final con la administración de la entidad u órgano auditado y con los responsables de poner en práctica las recomendaciones o disposiciones, antes de emitir el Informe Definitivo, con el fin de exponer los resultados, conclusiones y disposiciones o recomendaciones de la auditoría, de conformidad con lo establecido en los objetivos y alcance del proyecto, que ya conocen los interesados.

El informe de auditoría contiene un resumen ejecutivo de los principales resultados obtenidos, así como de las conclusiones, disposiciones o recomendaciones emitidas.

Las recomendaciones contemplan al menos lo siguiente: a) Generar valor a la entidad b) Atacar las causas del problema o condición identificada, c) Dirigidas al nivel responsable de solventar la deficiencia y d) Ser claras, específicas, convincentes y relevantes.

Entregables en esta etapa

- **Informe definitivo.** Debe incorporar las observaciones de la administración a cada hallazgo, observación o recomendación, si lo evidenciaron suficientemente.
- **Acta de reunión de comunicación de resultados.** Contiene los datos de fecha, hora inicio y fin; participantes convocados y presentes (con firma), observaciones y comentarios con nombre completo y puesto.
- **Recibido conforme de la institución.** Documento emitido por la misma persona que autorizó la realización del evento con firma de persona contacto (cuando fuese diferente). Indicando el cumplimiento de lo acordado y el grado de satisfacción con el trabajo.

Todo lo anterior apegado a la norma 210 “Calidad en la Auditoría”, que establece:

> El aseguramiento de la calidad de la auditoría es una labor que debe ejecutarse durante cada una de las actividades del proceso de auditoría, con el propósito de asegurar que los insumos, las tareas realizadas y los productos generados cumplan oportunamente con los estándares profesionales y con los requerimientos establecidos en la normativa bajo un enfoque de efectividad y mejoramiento continuo. (CGR, 2014)

CAPÍTULO 2- PERSPECTIVAS TEÓRICAS

2.1 Estado de la cuestión en Costa Rica

El tema de gobernanza de las tecnologías de información ha tomado mayor relevancia en los últimos años en Costa Rica, principalmente motivado por la decisión que tomó la Organización para la Cooperación y el Desarrollo Económicos (OCDE), en el año 2015, de invitar a Costa Rica a iniciar el proceso formal de adhesión, situación que llevó al país a diseñar una hoja de ruta con el objetivo de formar parte de este grupo.

Dentro de los temas que debe mejorar Costa Rica está el relacionado con los sistemas de gobierno corporativo y por ende, la forma de gobernar las tecnologías de información; a pesar de que durante años, el tema se ha promovido, aún se identifican oportunidades de mejora.

Los esfuerzos por fomentar este tema en relación con la normativa aplicable, han sido impulsados principalmente por el Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF) y la Contraloría General de la República (CGR), con la emisión del Reglamento sobre la Gestión de la Tecnología de Información SUGEF 14-09 en el 2009, mismo que fue derogado en el año 2017 con la emisión del Reglamento General de Gestión de la Tecnología de Información SUGEF 14-17, de aplicación para las superintendencias del país, el cual establece en su artículo 7:

> Las entidades supervisadas deben establecer una estructura de gobierno de TI con actividades y propósitos orientados a la generación de valor, a la consecución de beneficios acorde a los niveles de riesgo aceptables y al uso óptimo de los recursos de las tecnologías de la información.
>
> Las entidades supervisadas deben procurar que las necesidades de las partes interesadas sean evaluadas respecto a las metas corporativas

> establecidas; instituir una dirección del gobierno y de la gestión de TI priorizada; y asegurar que sea monitoreado el rendimiento y el cumplimiento respecto a la dirección y las metas acordadas.

La Contraloría General de la República, desde el 2007, emitió las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, en las cuales a pesar de que no incluye explícitamente el tema, demarcan la planeación estratégica de TI en su artículo 1:

> El jerarca debe traducir sus aspiraciones en materia de TI en prácticas cotidianas de la organización, mediante un proceso continuo de promulgación y divulgación de un marco estratégico constituido por políticas organizacionales que el personal comprenda y con las que esté comprometido.

Adicionalmente, existen diversos estándares en el mercado que han tomado terreno en el país, como COBIT, ITIL y normas ISO, que en parte o en su totalidad son utilizados como mejores prácticas para la gestión de las tecnologías, tanto para la empresa pública como para la privada.

La dependencia a las tecnologías de información que las empresas enfrentan día con día, y los retos que enfrentan los negocios, pone cada vez mayor evidencia de la necesidad de procesos robustos de gobierno de tecnologías y nuestro país no es ajeno a esta situación.

2.2 Historia de la empresa

La empresa donde se desarrolla el trabajo es una asociación que nació como un proyecto de responsabilidad social empresarial de una empresa privada desde el año 2009 y fue incubado como una unidad de negocio durante seis años, mismos que le permitieron madurar su modelo de negocio y posicionarse en el mercado, de forma que en el 2015 se transformó en una asociación sin fines de lucro, independizando su operación.

Este proceso de independencia le ha provocado enfrentar retos en su operación, debido a que procesos de soporte en su cadena de valor que antes eran liderados corporativamente por la empresa privada, como tecnologías de información, tuvo que asumirlos y soportarlos con personal interno y externo. Estos retos los ha enfrentado en una época en la cual el mercado que atiende y su estrategia los ha llevado a incorporar la tecnología en sus productos mediante el desarrollo de productos web, aplicaciones, realidad aumentada y cambios en sus sistemas de soporte administrativos.

Su filosofía de operación se resume mediante el establecimiento de su visión, misión y objetivos los cuales se detallan a continuación:

Visión

> Ser la asociación costarricense que, para el año 2020, beneficia a 100 000 niños de las áreas más vulnerables del sector educativo.

Misión

> Ofrecemos al sector educativo costarricense recursos didácticos de calidad y accesibles económicamente para el fortalecimiento de los procesos de aprendizaje de los estudiantes y el apoyo a la gestión docente.

Objetivos

- ➜ Ofrecer al sector educativo recursos didácticos de calidad y económicamente accesibles, que fortalezcan los procesos de aprendizaje de los estudiantes del sistema educativo costarricense y que apoyen la gestión docente.
- ➜ Crear y fomentar un espíritu de generosa colaboración principalmente a favor de la educación de los niños en Costa Rica.

Los productos que ofrece esta asociación abarcan servicios educativos y accesibles para la población que incluye libros de texto de Español, Matemática, Estudios Sociales y Ciencias; adicionalmente ofrece materiales complementarios de lectura y capacitación docente, para padres e hijos mediante su página web.

Una parte fundamental de su rol consiste en realizar campañas de donación por parte de empresas y personas físicas, para proveer a escuelas de bajos recursos de estos productos educativos. Para el año 2017, su principal logro fue proveer a 1020 escuelas de libros de texto para estudiar.

En relación con la gestión de tecnologías de información, ésta es liderada directamente por la Gerencia General y no se ha instaurado formalmente un departamento de tecnologías de información, trabajando principalmente con proveedores externos y soportando actividades del proceso con recurso interno, situación que poco a poco va mostrando síntomas de debilitamiento y alertas en su operación.

2.3 Normativa asociada

El trabajo de auditoría requiere criterios y normativa que permitan identificar mejores prácticas para ejecutar la evaluación del proceso, proporcionando objetividad al proceso de auditoría efectuado.

A continuación se detallan las principales normas que serán utilizadas como mejores prácticas para el proceso de gobierno de TI, en virtud de que la organización no cuenta con este tipo de normativa propia y tampoco le aplica la regulación que sí solicita este tema de manera vinculante.

COBIT 5.0 EDM01: Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno

> Proporcionar un enfoque consistente, integrado y alineado con el alcance del gobierno de la empresa. Para garantizar que las decisiones relativas a TI se han adoptado en línea con las estrategias y objetivos de la empresa, garantizando la supervisión de los procesos de manera efectiva y transparentemente, el cumplimiento con los requerimientos regulatorios y legales y que se han alcanzado los requerimientos de gobierno de los miembros del Consejo de Administración.

ISO/IEC 38500:2008: Esta norma proporciona estándares y mejores prácticas para el gobierno de las tecnologías de información; de acuerdo con la Asociación de Auditoría y Control de Sistemas de Información (ISACA) esta norma se puede resumir en tres propósitos fundamentales:

> Asegurar que, si la norma es seguida de manera adecuada, las partes implicadas (directivos, consultores, ingenieros, proveedores de hardware, auditores, etc.), puedan confiar en el gobierno corporativo de TIC.
>
> Informar y orientar a los directores que controlan el uso de las TIC en su organización.
>
> Proporcionar una base para la evaluación objetiva por parte de la alta dirección en el gobierno de las TIC.

2.4 Estudio preliminar

El gobierno de las tecnologías de información en una transformación como la que está enfrentando esta asociación puede estar propenso a un debilitamiento, debido a que estructuras de alineamiento y gobierno sufren cambios significativos, tanto a nivel de personas como experiencia, en este caso específico, la administración de la asociación se enfrenta a pasar de mantener una dirección de Junta Directiva corporativa a la conformación de una nueva Junta Directiva propia.

Anudado a esto la gestión de nuevos roles dentro de la administración que en el pasado fueron dictados corporativamente se deben reestructurar y adaptarse al nuevo entorno, como lo es pasar de contar con un departamento de tecnologías de información que atendía todo el negocio bajo lineamientos corporativos a tener que definir cómo soportaría la gestión de las TI a partir del proceso de separación.

Sin la dirección adecuada, estas adaptaciones y cambios pueden provocar que la operativa de la asociación y la atención a su negocio hagan que algunos

procesos pasen a un plano operativo y no estratégico, como lo son las tecnologías de información.

Adicionalmente, la necesidad de mantener una estructura de bajo costo que le permita a la asociación cumplir con su misión y metas establecidas es un componente más que pone en riesgo la gobernanza de procesos de esta naturaleza.

CAPÍTULO 3- DESARROLLO DEL TEMA DE INVESTIGACIÓN

3.1 Actividades del Proyecto

El proyecto se efectúa según las etapas planteadas en la metodología, iniciando con la planificación; posteriormente se desarrollará la ejecución o examen y por último, la comunicación de resultados. A continuación, se describe cada una de ellas.

3.1.1 Etapa 1- Planificación

Esta etapa inicia con un estudio preliminar con el propósito de tener claro el objetivo, naturaleza de la empresa, así como conocer las necesidades y el ambiente de control donde se desarrolla la auditoría.

Producto de la anterior indagación se determina la oportunidad y posibilidad real de llevar a cabo el trabajo con el alcance y en el tiempo establecido, así como los recursos requeridos.

Una vez determinada la viabilidad de cumplir con los objetivos del proyecto y de la empresa, se prepara el programa de ejecución del trabajo, para que una vez aprobado se comiencen a determinar las áreas de riesgo, diseñar las herramientas para atender de extremo a extremo todo el programa de ejecución, diseñar el mapa de riesgos, diseñar las pruebas, los cuestionarios, las guías de entrevista y todas las plantillas de trabajo para evidenciar su ejecución.

3.1.2 Programa de examen del proyecto

En programa de examen, se definen los procedimientos de auditoría que se requieren aplicar para cumplir con los objetivos del proyecto; así como el objetivo, naturaleza, alcance, oportunidad, plazo y responsables de éstos. (CGR, 2014)

En virtud de lo anterior se describe a continuación el programa para ejecutar la auditoría de gobierno de las tecnologías de información:

Proceso a Auditar:	Gobierno de tecnologías de información		
Responsable:	Carmen Murillo Murillo		
Aprobado por:			
	MSc. Marco V. Gámez Acuña	Firma	Fecha
Plazo de ejecución	De noviembre 2017 a abril 2018		

Objetivos de la auditoría

Realizar una evaluación del gobierno de las tecnologías de información de una asociación sin fines de lucro.

Alcance

Actuaciones de la asociación privada sin fines de lucro en relación con el proceso de gobierno de las tecnologías de información, comprendidas entre los meses de enero-diciembre de 2017.

Procedimientos de trabajo

Procedimientos por ejecutar			
ID	**Detalle**	**Ref. PT**	**Tiempo estimado**
A	**Determinación del alcance de la iniciativa de aseguramiento**		
A.1	Determine las partes interesadas en el gobierno de las tecnologías de información y el rol de cada una de éstas.		
A.2	Determine los objetivos de aseguramiento para el gobierno de las tecnologías de información basados en la evaluación del entorno / contexto interno y externo y del riesgo relevante y las oportunidades relacionadas.		
A.3	Determine los habilitadores y la (s) instancia (s) de los habilitadores en el alcance del gobierno de las tecnologías de información.		
B	**Comprender habilitadores, establecer criterios de evaluación adecuados y realizar la evaluación**		

B-1	Acuerde con las partes interesadas según su rol las métricas y los criterios para los objetivos empresariales y los objetivos relacionados con TI.		
B-2	Obtenga la comprensión del proceso de gobierno de las tecnologías de información y establezca los criterios de evaluación adecuados.		
B-3	Obtenga una comprensión de los Principios, Políticas y Marcos de referencia para el gobierno de las tecnologías de información y evalúelos contra los criterios definidos previamente.		
B-4	Obtenga comprensión de las estructuras organizacionales relacionadas con el gobierno de las tecnologías de información y evalúelas contra los criterios definidos previamente.		
B-5	Obtenga una comprensión de la Cultura, la Ética y el Comportamiento relacionados con el gobierno de las tecnologías de información y evalúelos contra los criterios definidos previamente.		
B-6	Obtenga una comprensión de los ítems de información relacionados con el gobierno		

	de las tecnologías de información y evalúelos contra los criterios definidos previamente.		
B-7	Obtenga una comprensión de los Servicios, Infraestructura y Aplicaciones relacionados con el gobierno de las tecnologías de información y evalúelos contra los criterios definidos previamente.		
B-8	Obtenga comprensión de las Personas, Habilidades y Competencias relacionadas con el gobierno de las tecnologías de información y evalúelos contra los criterios definidos previamente.		
C	**Comunica los resultados de la evaluación**		
C-1	Documente excepciones y brechas		
C-2	Comunique el trabajo realizado y los hallazgos.		

3.2 Examen o ejecución

La ejecución del proceso de auditoría se inició una vez aprobado el programa de examen del proyecto incluido en el apartado anterior, posteriormente se realizó el cronograma de actividades detallado[1], en éste se describen las tareas a desarrollar para cumplir con cada procedimiento a ejecutar del programa, cabe aclarar que un proyecto de auditoría de tecnologías de información, así como un proyecto de otra naturaleza, requiere la gestión de los recursos asignados, por lo cual mediante esta herramienta se asignaron las horas requeridas para completar cada tarea, definiendo la fecha estimada de conclusión del proyecto y utilizada a lo largo de todo el proceso para identificar desviaciones en lo planificado que pudieran afectar la conclusión a satisfacción del proyecto.

3.2.1 Determinación del alcance de la iniciativa de aseguramiento

La determinación del alcance de la iniciativa de aseguramiento consta de tres grandes procedimientos según se detalló en el programa de examen para los cuales se aplicaron tareas específicas para cumplir con cada uno según se describe a continuación:

- ➔ Determine las partes interesadas en el gobierno de las tecnologías de información y el rol de cada una de éstas.

La determinación de las partes interesadas en el gobierno de las TI se realizó utilizando la plantilla Usuarios previstos para el informe[2], mediante el cual se documentó el entendimiento de la estructura organizacional, solicitando el organigrama vigente de la empresa y documentando los roles del personal clave identificado en este organigrama mediante entrevistas con la Gerencia de la Asociación. Con esta información como insumo se procedió a completar el

[1] Plantilla incluida en punto 4.2 del capítulo 4.
[2] Plantilla incluida en punto 4.3 del capítulo 4.

formulario Matriz RACI[3], para lo cual se utilizaron los subprocesos de COBIT 5 "EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno", identificando el rol que ejercen las partes interesadas de la Asociación para cada subproceso y asignando los tipos de responsabilidad definidos por esta matriz a saber; responsable, quien rinde cuentas, consultado e informado.

- ➔ Determine los objetivos de aseguramiento para el gobierno de las tecnologías de información basados en la evaluación del entorno / contexto interno y externo y del riesgo relevante y las oportunidades relacionadas.

Para determinar los objetivos de aseguramiento para el gobierno de las TI se utilizó la plantilla Entendimiento de la entidad[4], la cual consta de cinco apartados, iniciando con el entendimiento general de la entidad que incluye su estructura legal, normas legales aplicables, su cadena de valor, objetivos y estrategia, sistemas de información, clientes, proveedores, productos, etc., continúa con un entendimiento de los factores del ambiente externo que permitan identificar riesgos ambos insumos le permiten al auditor identificar los factores externos e internos que podrían influir en el proceso de auditoría e identificar las prioridades estratégicas y relacionarlos con objetivos concretos para el proceso de auditoría, finalizando con la definición de las entidades o la entidad que cubre el proceso de auditoría.

- ➔ Determine los habilitadores y la (s) instancia (s) de los habilitadores en el alcance del gobierno de las tecnologías de información.

Para cubrir esta tarea se utilizó la plantilla Alcance de habilitadores[5], mediante la cual se define el proceso que abarca el alcance de la revisión utilizando la definición que proporciona COBIT 5 del "EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno" y además basándose en el

[3] Plantilla incluida en punto 4.4 del capítulo 4.
[4] Plantilla incluida en punto 4.5 del capítulo 4.
[5] Plantilla incluida en punto 4.6 del capítulo 4.

entendimiento, objetivos y factores identificados en el punto anterior se delimitaron los habilitadores de mayor impacto que se desarrollarán en el proceso de revisión, es importante que siempre se recomienda cubrir los siete habilitadores de COBIT 5, pero esto va depender del nivel de recursos y el nivel de riesgo identificado. Un habilitador según lo define COBIT 5 son factores que influyen sobre si algo funcionará, en nuestro alcance sería el gobierno de las TI. COBIT 5 describe siete habilitadores:

- ➔ Principios, políticas y marcos de referencia: proporciona guías para la gestión del día a día de las organizaciones esto mediante lineamientos que determinan el comportamiento deseado.
- ➔ Procesos: conjunto de actividades y prácticas para alcanzar objetivos de TI y generar un resultado o salida.
- ➔ Las estructuras organizativas: define línea de mando y toma de decisión.
- ➔ La cultura, ética y comportamiento: lineamientos que guían el comportamiento y la toma de decisiones en una organización.
- ➔ La información: corresponde a la información producida para operar y gobernar las organizaciones.
- ➔ Los servicios, infraestructuras y aplicaciones: corresponde a la infraestructura, tecnología y aplicaciones que brindan servicios y tecnologías de procesamiento de la información a las organizaciones.
- ➔ Las personas, habilidades y competencias: están relacionadas con las personas y son necesarias para poder completar de manera satisfactoria todas las actividades y para la correcta toma de decisiones y de acciones correctivas.

3.2.2 Comprender habilitadores, establecer criterios de evaluación adecuados y realizar la evaluación

Una vez definidos los habilitadores incluidos en el alcance se elaboraron cuestionarios para cada habilitador, que permitiera obtener un entendimiento para establecer los criterios de evaluación a utilizar. Es importante mencionar que el cuestionario de cada habilitador se desarrolló basado en las dimensiones comunes de los habilitadores de COBIT 5, según la siguiente estructura:

- ➔ Partes interesadas: cada habilitador tiene partes interesadas que pueden ser internas o externas, estas tienen diferentes necesidades que se traducen en metas corporativas que tienen relacionados objetivos de TI.
- ➔ Metas: son los resultados esperados de cada habilitador.
- ➔ Ciclo de Vida: los habilitadores tienen un ciclo de vida desde su inicio con la planificación, diseño, implementación, operación, evaluación hasta su eliminación.
- ➔ Buenas prácticas: estas son un mecanismo que permite el logro de los objetivos del habilitador, son estándares y marcos de referencia.

Para cada habilitador se desarrolló un cuestionario sobre cada dimensión[6], adicionalmente, se reforzó el cuestionario basado en las actividades del proceso EDM01 de COBIT 5, incorporando preguntas sobre los principios de gobierno establecidos en ISO/IEC 38500:2008, estos fueron aplicados a la Gerencia de la Asociación.

Al aplicar los diferentes cuestionarios se determinó que existen limitaciones significativas en relación con el establecimiento de los criterios de evaluación debido a las deficiencias que permitieron identificar las respuestas a los cuestionarios, por lo cual se inició con la documentación de los resultados.

[6] Plantillas de cuestionarios incluidas en los puntos del 4.8 al 4.12 del capítulo 4.

3.3 Comunicación de resultados

Por un requerimiento de confidencialidad acordado con la Asociación previo al inicio de este trabajo de investigación, y de acuerdo con lo establecido en los términos para su realización desde el inicio del curso Práctica Profesional I, no resulta factible incluir en este apartado los resultados logrados o hallazgos determinados; los cuales fueron ampliamente detallados en el informe entregado a las autoridades de la Asociación según consta en acta ACT-AUD-01 y fueron expuestos a esas instancias según se indica a continuación:

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	ACT-AUD-01
	Versión: 01
ACTA DE CONFERENCIA DEL INFORME DE AUDITORIA	

El día **22 de marzo de 2018,** en las oficinas de la asociación sin fines de lucro, se realizó la conferencia del "Informe de auditoría sobre Gobierno de las Tecnologías de Información", correspondiente a la actividad realizada del Trabajo Final de Graduación de la Maestría Profesional en Auditoría de Tecnologías de Información, los abajo firmantes manifiestan haber participado en dicha conferencia estando en acuerdo con los temas tratados

PARTICIPANTE	PUESTO	FIRMA
Hanie Cordero Calderón	Gerente de Operaciones	
Carmen Murillo Murillo	Sustentante	

Lo anterior no obsta para mencionar que se determinaron una serie de condiciones relevantes que la empresa auditada dio por aceptadas y se comprometió a iniciar a la mayor brevedad las tareas necesarias para fortalecer las estructura de control que garanticen la adecuada gobernanza de las TI; las cuales se mencionan en términos generales en el capítulo 5.

3.4 Evidencia de Auditoría

Para la toma de la evidencia se utilizaron diferentes técnicas de auditoría entre ellas se encuentran:

Plantillas de trabajo: Se realizaron diferentes formularios con el fin de recopilar información y evaluar condiciones específicas. Las plantillas utilizadas se pueden encontrar en el capítulo cuatro de este documento.

Análisis de contenido: Se efectuó un análisis de la información recopilada mediante la aplicación de las plantillas de trabajo, que permitió obtener los resultados del proyecto.

Entrevistas: Aplicadas al personal relacionado con el gobierno de las TI y documentadas mediante minutas formales.

3.5 Documentación de la Auditoría

La Asociación solicitó confidencialidad en la información recopilada en el proceso de auditoría, es por esta razón que en este documento no se incluye la documentación del proceso aplicado, pero cabe recalcar que ésta se llevó a cabo con las plantillas adjuntas en este documento y bajo proceso de su revisión de calidad. Una copia del expediente que incluye la totalidad de esta evidencia fue suministrada a las autoridades de la Asociación.

3.6 Calidad en la Auditoría

El proceso de auditoría se desarrolló bajo estos principios de calidad:

- ➔ Ética: el trabajo fue desarrollado bajo los principios de ética establecidos por el Instituto de Auditores Internos de Costa Rica.
- ➔ Supervisión: la supervisión del trabajo ejecutado estuvo a cargo del tutor del proyecto.
- ➔ Basada en mejores prácticas: el proceso fue ejecutado guiado por el estándar COBIT 5 y además se utilizaron herramientas emitidas por ISACA como lo fue el programa de auditoría sugerido para el proceso EDM01.

CAPÍTULO 4- PLANTILLAS DE HOJAS O PAPELES DE TRABAJO

El desarrollo de este proyecto busca proveer de papeles de trabajo base que puedan ser utilizados para la elaboración de una auditoría de gobierno de las TI, por lo cual a continuación se detallan los documentos utilizados en el proceso de auditoría actual.

4.1 Programa de Examen del Proyecto

El programa de examen del proyecto es el documento inicial de planificación en el cual se definen los procedimientos de auditoría que se requieren aplicar para cumplir con los objetivos correspondientes.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

REF _____

TRABAJO FINAL DE GRADUACIÓN

Proceso a Auditar:	**Gobierno de tecnologías de información**		
Responsable:			
Aprobado por:			
	Nombre	Firma	Fecha
Plazo de ejecución			

Objetivos de la auditoría

Realizar una evaluación del gobierno de las tecnologías de información de (indicar la empresa).

Alcance

Delimitar en tiempo y entidades que el proyecto de auditoría abarca.

Procedimientos de trabajo

ID	Detalle	Ref. PT	Tiempo estimado
A	**Determinación del alcance de la iniciativa de aseguramiento**		
A.1	Determine las partes interesadas en el gobierno de las tecnologías de información y el rol de cada una de éstas.		
A.2	Determine los objetivos de aseguramiento para el gobierno de las tecnologías de información basados en la evaluación del entorno / contexto interno y externo y del riesgo relevante y las oportunidades relacionadas.		
A.3	Determine los habilitadores y la (s) instancia (s) de los habilitadores en el alcance del gobierno de las tecnologías de información.		
B	**Comprender habilitadores, establecer criterios de evaluación adecuados y realizar la evaluación**		

B-1	Acuerde con las partes interesadas según su rol las métricas y los criterios para los objetivos empresariales y los objetivos relacionados con TI.		
B-2	Obtenga la comprensión del proceso de gobierno de las tecnologías de información y establezca los criterios de evaluación adecuados.		
B-3	Obtenga una comprensión de los Principios, Políticas y Marcos de referencia para el gobierno de las tecnologías de información y evalúelos contra los criterios definidos previamente.		
B-4	Obtenga comprensión de las estructuras organizacionales relacionadas con el gobierno de las tecnologías de información y evalúelas contra los criterios definidos previamente.		
B-5	Obtenga una comprensión de la Cultura, la Ética y el Comportamiento relacionados con el gobierno de las tecnologías de información y evalúelos contra los criterios definidos previamente.		
B-6	Obtenga una comprensión de los ítems de información relacionados con el gobierno de las tecnologías de información y evalúelos contra los criterios definidos previamente.		

B-7	Obtenga una comprensión de los Servicios, Infraestructura y Aplicaciones relacionados con el gobierno de las tecnologías de información y evalúelos contra los criterios definidos previamente.		
B-8	Obtenga comprensión de las Personas, Habilidades y Competencias relacionadas con el gobierno de las tecnologías de información y evalúelos contra los criterios definidos previamente.		
C	**Comunica los resultados de la evaluación**		
C-1	Documente excepciones y brechas		
C-2	Comunique el trabajo realizado y los hallazgos.		

4.2 Cronograma de actividades

El cronograma de actividades se convierte en una herramienta relevante de seguimiento de un proyecto, el objetivo de este papel de trabajo es identificar y definir cada una de las actividades que componen el proyecto de auditoría y distribuir temporalmente su realización.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

TRABAJO FINAL DE GRADUACIÓN

REF _____

PAPEL DE TRABAJO

Objetivo

El objetivo de este papel de trabajo es identificar y definir cada una de las actividades que componen el proyecto de auditoría y distribuir temporalmente su realización.

Este es un modelo que debe ser adecuado a las características particulares de cada entidad.

Contenido

1. Cronograma de actividades

Aplicabilidad

Este papel de trabajo deberá ser completado y revisado en su totalidad.

Evidencia de Revisión

Como evidencia de revisión, este papel de trabajo debe ser firmado por quien lo realizó y revisó.

Nombre		Fecha (dd/mm/aaaa):	Firma
Elaboró:			
Revisó:			

Cronograma de trabajo detallado

Nivel	Tarea	Responsable	Start	Final	Duración	% Complete
1	Determinación del alcance de la iniciativa de aseguramiento					
2	**Determine las partes interesadas en el gobierno de las tecnologías de información y el rol de cada una de éstas.**					
3	Identifique el (los) usuario (s) previsto (s) del informe de auditoría y su participación en el proceso de auditoría. Describa los usuarios del informe de auditoría y sus roles.					
3	Identifique a las partes interesadas, responsables y responsables del gobierno de ls tecnologías de TI.					
2	**Determine los objetivos de aseguramiento para el gobierno de las tecnologías de información basados en la evaluación del entorno / contexto interno y externo y del riesgo relevante y las oportunidades relacionadas.**					
3	Comprenda la estrategia y las prioridades de la empresa. Consulte con la gerencia general sobre la estrategia y las prioridades de la empresa para el próximo período, y documente en la medida en que el proceso bajo revisión sea relevante.					
3	Comprenda el contexto interno de la empresa. Identifique todos los factores internos que podrían influir en el desempeño del proceso bajo revisión.					
3	Comprender el contexto externo de la empresa. Identifique todos los factores externos que podrían influir en el desempeño del proceso bajo revisión.					
3	Traduzca las prioridades estratégicas identificadas en objetivos concretos para el proceso de auditoría.					
3	Definir los límites organizacionales de la iniciativa de aseguramiento. Describa las entidades que cubre el proceso de auditoría.					
2	**Determine los habilitadores y la (s) instancia (s) de los habilitadores en el alcance del gobierno de las tecnologías de información.**					
3	Definir el proceso en el alcance de la revisión.					
3	Defina los habilitadores relacionados. Los habilitadores relacionados incluyen los 7 habilitadores definidos por COBIT 5.					
1	**Comprender habilitadores, establecer criterios de evaluación adecuados y realizar la evaluación**					
2	**Acuerde con las partes interesadas según su rol, las métricas y los criterios para los objetivos empresariales y los objetivos relacionados con TI.**					
3	Obtenga (y acuerde) métricas para las metas de la empresa y los valores esperados de las métricas y evalúe si se logran los objetivos empresariales en el alcance.					
3	Obtenga (y acuerde) métricas para objetivos relacionados con TI y valores esperados de las métricas y evalúe si se logran objetivos relacionados con TI en el alcance.					
2	**Obtenga la comprensión del proceso de gobierno de las tecnologías de información y establezca los criterios de evaluación adecuados.**					
3	Comprenda el propósito del proceso.					
3	Comprenda los objetivos del proceso y las métricas relacionadas y definir los valores esperados (criterios), y evaluar si se logran los objetivos del proceso (resultados), es decir, evaluar la eficacia del proceso.					
3	Identifique las entradas y salidas del proceso y evalúe en qué medida están disponibles los productos de trabajo de proceso.					
3	Acordar el nivel de capacidad del proceso que se logrará mediante la ejecución del proceso.					
2	**Obtenga una comprensión de los Principios, Políticas y Marcos de referencia para el gobierno de las tecnologías de información y evalúelos contra los criterios definidos previamente.**					
3	Obtenga una comprensión del sistema general de control interno y los Principios, Políticas y Marcos asociados.					

Nivel	Tarea	Responsable	Start	Final	Duración	% Complete
3	Obtenga un entendimiento de los interesados en las políticas. Los interesados en las políticas incluyen aquellos que establecen las políticas y aquellos que necesitan cumplir con las políticas.					
3	Evaluar si se logran los objetivos de los Principios, Políticas y Marcos, es decir, evaluar la efectividad de los Principios, Políticas y Marcos.					
3	Obtenga un entendimiento general de las etapas del ciclo de vida de los Principios, Políticas y Marcos, y acordar los criterios relevantes. Evaluar en qué medida se gestiona el ciclo de vida de Principios, Políticas y Marcos.					
3	Comprenda las buenas prácticas relacionadas con los Principios, Políticas y Marcos, y los valores esperados. Evalue el diseño de Principios, Políticas y Marcos, es decir, evaluar en qué medida se aplican las buenas prácticas esperadas.					
2	**Obtenga comprensión de las estructuras organizacionales relacionadas con el gobierno de las tecnologías de información y evalúelas contra los criterios definidos previamente.**					
3	Identifique y documente todos los elementos que pueden ayudar a comprender el contexto en el cual la Estructura organizacional					
3	Determine a través de la revisión de la documentación (políticas, comunicaciones de gestión, etc.) las partes interesadas clave					
3	Comprenda los objetivos de la Estructura Organizativa, las métricas relacionadas y acuerde los valores esperados. Comprenda cómo estos objetivos contribuyen al logro de los objetivos de la empresa y los objetivos relacionados con TI.					
3	Acuerde las buenas prácticas esperadas para la Estructura Organizativa contra la cual se evaluará. Evalué el diseño de la Estructura Organizativa, es decir, evaluar en qué medida se aplican las buenas prácticas esperadas.					
3	Evalúe la medida en que se gestiona el ciclo de vida de la Estructura Organizativa.					
2	**Obtenga una comprensión de la Cultura, la Ética y el Comportamiento relacionados con el gobierno de las tecnologías de información y evalúelos contra los criterios definidos previamente.**					
3	Comprender el contexto de Cultura, Ética y Comportamiento. Cómo es la cultura corporativa general					
3	Comprenda a quién se aplicarán los requisitos de comportamiento. Esto generalmente está vinculado a los roles y las estructuras organizacionales identificadas en el alcance.					
3	Evaluar si se logran los objetivos de Cultura, Ética y Comportamiento (resultados), es decir, evaluar la efectividad de Cultura, Ética y Comportamiento.					
3	Evalúe en qué medida se gestiona el ciclo de vida de Cultura, Ética y Comportamiento.					
3	Evaluar el diseño de Cultura, Ética y Comportamiento, es decir, evaluar en qué medida se aplican las buenas prácticas esperadas.					
2	**Obtenga una comprensión de los ítems de información relacionados con el gobierno de las tecnologías de información y evalúelos contra los criterios definidos previamente.**					
3	Comprender el contexto del elemento de información					
3	Comprender las partes interesadas para el elemento Información					
3	Evaluar si se logran los criterios de calidad de elementos de información (resultados), es decir, evaluar la efectividad del elemento Información.					
3	Evalúe en qué medida se gestiona el ciclo de vida del elemento Información.					
3	Evaluar el diseño del elemento de Información, es decir, evaluar en qué medida se aplican las buenas prácticas esperadas.					
2	**Obtenga una comprensión de los Servicios, Infraestructura y Aplicaciones relacionados con el gobierno de las tecnologías de información y evalúelos contra los criterios definidos previamente.**					

Nivel	Tarea	Responsable	Start	Final	Duración	% Complete
3	Comprender el contexto de Servicios, Infraestructura y Aplicaciones.					
3	Comprenda quiénes serán los principales interesados del servicio, es decir, el patrocinador, el proveedor y los usuarios. Las partes interesadas incluirán una serie de funciones organizacionales, pero también podrían vincularse a los procesos.					
3	Evaluar si se logran los objetivos de Servicios, Infraestructura y Aplicaciones (resultados), es decir, evaluar la efectividad de los Servicios, la Infraestructura y las Aplicaciones.					
3	Evalúe en qué medida se gestiona el ciclo de vida de Servicios, Infraestructura y Aplicaciones.					
3	Evaluar el diseño de Servicios, Infraestructura y Aplicaciones, es decir, evaluar en qué medida se aplican las buenas prácticas esperadas.					
2	**Obtenga comprensión de las Personas, Habilidades y Competencias relacionados con el gobierno de las tecnologías de información y evalúelos contra los criterios definidos previamente.**					
3	Comprender el contexto de Personas, Habilidades y Competencias.					
3	Comprender a los principales interesados para las personas, las habilidades y las competencias.					
3	Evaluar si se logran los objetivos, los resultados, las personas, las habilidades y las competencias, es decir, evaluar la efectividad de las personas, las habilidades y las competencias.					
3	Evaluar en qué medida se gestiona el ciclo de vida Personas, Habilidades y Competencias.					
3	Evaluar el diseño de Personas, Habilidades y Competencias, es decir, evaluar en qué medida se aplican las buenas prácticas esperadas.					
1	Comunica los resultados de la evaluación					
2	**Documente excepciones y brechas.**					
3	Comprender y documentar las debilidades y su impacto en el logro de los objetivos del proceso.					
3	Comprender y documentar las debilidades y su impacto en los objetivos de la empresa.					
2	**Comunique el trabajo realizado y los hallazgos.**					
3	Elaborar y circular informe borrador					
3	Elaborar y circular informe final					

4.3 Usuarios previstos para el informe

El objetivo de este papel de trabajo es documentar las partes interesadas en el gobierno de las tecnologías de información y el rol de cada una de éstas.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

REF ____

TRABAJO FINAL DE GRADUACIÓN

PAPEL DE TRABAJO

Objetivo

El objetivo de este papel de trabajo es documentar las partes interesadas en el gobierno de las tecnologías de información y el rol de cada una de éstas**.**
Este es un modelo que debe ser adecuado a las características particulares de cada entidad.

Contenido

2. Entendimiento estructura organizacional de la entidad
3. Entendimiento de roles de la entidad
4. Matriz RACI

Aplicabilidad

Este papel de trabajo deberá ser completado y revisado en su totalidad.

Evidencia de Revisión

Como evidencia de revisión, este papel de trabajo debe ser firmado por quien lo realizó y revisó.

Nombre		Fecha (dd/mm/aaaa):	Firma
Elaboró:			
Revisó:			

1. Entendimiento estructura organizacional de la entidad

Solicite el organigrama vigente de la empresa, que describa la estructura organizacional desde la Junta Directiva hasta el último nivel de la organización.

2. Entendimiento de roles de la entidad

Mediante entrevista con el más alto cargo de la administración obtenga entendimiento del rol de cada puesto.

Cargo/	Nombre	Rol
Junta Directiva		
Comité Estratégico		
Gerente Operativo		
Encargado de TI		
Editor Supervisor		
Encargada de procesos operativos		
Coordinador de donaciones		
Supervisor de canal de venta		
Editores de contenido		

3. Matriz RACI

Documente la matriz RACI utilizando como guía la matriz sugerida por el proceso EDM01 de COBIT 5, para lo cual se utiliza la herramienta, utilice papel de trabajo “Matriz RACI”

4.4 Matriz RACI

El objetivo de este papel de trabajo es documentar la asignación de responsabilidades de las partes interesadas en el gobierno de las tecnologías de información y el rol de cada una de éstas.

REF _____

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

TRABAJO FINAL DE GRADUACIÓN

PAPEL DE TRABAJO

Objetivo
El objetivo de este papel de trabajo es documentar las partes interesadas en el gobierno de las tecnologías de información y el rol de cada una de éstas.

Este es un modelo que debe ser adecuado a las características particulares de cada entidad.

Contenido
1. Matriz de Asignación de Responsabilidades (RACI, por las iniciales de los tipos de responsabilidad)

Aplicabilidad
Este papel de trabajo deberá ser completado y revisado en su totalidad.

Evidencia de Revisión
Como evidencia de revisión, este papel de trabajo debe ser firmado por quien lo realizó y revisó.

Nombre		Fecha (dd/mm/aaaa):	Firma
Elaboró:			
Revisó:			

Matriz RACI

La Matriz RACI se completa siguiendo los siguientes pasos:

- ➔ Identificar los subproceso de algún proceso de COBIT 5 (y colocarlas como filas de la matriz), en este caso utilizamos los subprocesos del EDM01.
- ➔ Identificar / definir los principales roles funcionales (y colocarlos como columnas de la matriz).
- ➔ Asignar los códigos “RACI” a cada subproceso.

Práctica Clave de Gobierno	Junta Directiva	Gerente Operativo	Encargado procesos operativos	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Encargado de TI	Editor Supervisor	Editores de contenido
EDM01.01 **Evaluar el sistema de gobierno:** Identificar y comprometerse continuamente con las partes interesadas de la empresa, documentar la comprensión de los requerimientos y realizar una estimación del actual y futuro diseño del gobierno de TI de la empresa.								
EDM01.02 **Orientar el sistema de gobierno:** Informar a los líderes y obtener su apoyo, su aceptación y su compromiso. Guiar las estructuras, procesos y prácticas para el gobierno de TI en línea con los principios, modelos para la toma de decisiones y niveles de autoridad diseñados para el gobierno. Definir la información necesariapara una toma de decisiones informadas.								
EDM01.03 **Supervisar el sistema de gobierno:** Supervisar la ejecución y la efectividad del gobierno de TI de la empresa. Analizar si el sistema de gobierno y los mecanismos implementados (incluyendo estructuras, principios y procesos) están operando de forma efectiva y proporcionan una supervisión apropiada de TI.								

Significado de los tipos de responsabilidad:

R (Responsible): Este rol corresponde a quien efectivamente realiza la tarea. Lo más habitual es que exista sólo un encargado (R) por cada tarea; si existe más de uno, entonces el trabajo debería ser subdividido a un nivel más bajo, usando para ello las matrices RACI.

A (Accountable): Este rol se responsabiliza de que la tarea se realice y es el que debe rendir cuentas sobre su ejecución. Sólo puede existir una persona que deba rendir cuentas (A) de que la tarea sea ejecutada por su Responsable (R).

C (Consulted): Este rol posee alguna información o capacidad necesaria para realizar la tarea.

I (Informed): Este rol debe ser informado sobre el avance y los resultados de la ejecución de la tarea. A diferencia del consultado (C), la comunicación es unidireccional.

4.5 Entendimiento de la entidad

Este papel de trabajo fue utilizado para documentar la información relevante que permitió determinar los objetivos de aseguramiento para el gobierno de las tecnologías de información basados en la evaluación del entorno / contexto interno y externo y del riesgo relevante y las oportunidades relacionadas.

REF _____

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

TRABAJO FINAL DE GRADUACIÓN

PAPEL DE TRABAJO

Objetivo

El objetivo de este papel de trabajo es documentar la información relevante para que el equipo de auditoría determine los objetivos de aseguramiento para el gobierno de las tecnologías de información basados en la evaluación del entorno / contexto interno y externo y del riesgo relevante y las oportunidades relacionadas

Este es un modelo que debe ser adecuado a las características particulares de cada entidad.

Contenido

1. Entendimiento general de la entidad.
2. Ambiente externo de la entidad.
3. Factores externo e interno de la entidad que podrían influir en el proceso de auditoría.
4. Prioridades estratégicas identificadas en objetivos concretos para el proceso de auditoría.
5. Definición de entidades que cubre el proceso de auditoría.

Aplicabilidad

Este papel de trabajo deberá ser completado y revisado en su totalidad.

Evidencia de Revisión

Como evidencia de revisión, este papel de trabajo debe ser firmado por quien lo realizó y revisó.

Nombre		Fecha (dd/mm/aaaa):	Firma
Elaboró:			
Revisó:			

1. Entendimiento general de la entidad

1.1. Negocio de la entidad

Para entender la entidad se deben realizar indagaciones en relación con los siguientes aspectos:

1.1.1. Objeto entidad

1.1.2. Sedes (Incluye oficina principal, plantas bodegas, etc.)

Descripción Sede	Localización	Actividad principal

1.1.3. Estructura legal

Representante legal

Nombre	Cargo

Junta Directiva

Nombre	Cargo

1.1.4. Normas generales y específicas que le aplican a la organización

Generales

Norma	Descripción	Periodicidad de Reportes

Normas específicas de la industria:

Norma	Descripción	Periodicidad de Reportes

1.1.5. Estructura operativa / Cadena de Valor

Se sugiere anexar un organigrama de la entidad, así como la cadena de valor, en caso de que la cadena de valor no esté diagramada obtenga un entendimiento y diagrame el proceso:

Cadena de Valor de LPT	
Organigrama de LPT	

1.1.6. Objetivos y estrategias del negocio

Dimensión ambiental

Objetivos	Estrategias

Dimensión Social

Objetivos	Estrategias

Dimensión económica

Objetivos	Estrategias

1.1.7. Sistemas de información de la entidad

Diagrama de sistemas de información

1.1.8. Clientes

Tipo de Clientes	Descripción de la Relación

1.1.9. Proveedores

Nombre del Proveedor	Descripción de la Relación

1.1.10. Empleados

Descripción de la Relación
No. Empleados:

1.1.11. Productos y Servicios

Descripción del los productos y servicios

1.1.12. Principales sistemas de información

El entendimiento de los sistemas de información se obtuvo así:

a. Estrategia de Sistemas de Información

b. Identificación de la infraestructura que soporta sistemas.

c. Cambios, proyectos o adquisiciones de sistemas

d. Procedimientos vigentes relacionados con sistemas de información

e. Contratos relacionados con sistemas de información

2. Ambiente externo de la entidad

2.1.1. Ambiente político, económico, social, tecnológico y ambiental.

Ambiente externo	Factores externos generadores de riesgos
Político	
Económico	
Social	
Tecnológico	
Ambiental	

3. Factores externo e interno de la entidad que podrían influir en el proceso

3.1. Factores internos que podrían influir en el desempeño del proceso bajo revisión.

3.2. Factores externos que podrían influir en el desempeño del proceso bajo revisión.

4. Prioridades estratégicas identificadas en objetivos concretos para el proceso de auditoría.

Basado en su entendimiento del negocio identifique las prioridades estratégicas y defina con la administración los Objetivos Corporativos de COBIT 5 relacionadas directamente con las prioridades estratégicas.

Posteriormente utilizando el apéndice B de COBIT 5 identifique los objetivos de TI que tengan una relación Primaria (P)

5. Definición de entidades que cubre el proceso de auditoría.

Indique las entidades que cubren el alcance del proyecto.

4.6 Alcance de habilitadores

El objetivo de este papel de trabajo es determinar los habilitadores a incluir en el alcance del gobierno de las tecnologías de información.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

REF ____

TRABAJO FINAL DE GRADUACIÓN

PAPEL DE TRABAJO

Objetivo

El objetivo de este papel de trabajo es determinar los habilitadores y la (s) instancia (s) de los habilitadores en el alcance del gobierno de las tecnologías de información.

Este es un modelo que debe ser adecuado a las características particulares de cada entidad.

Contenido

1. Definición del proceso que abarca el alcance de la revisión.
2. Definir los habilitadores relacionados.

Aplicabilidad
Este papel de trabajo deberá ser completado y revisado en su totalidad.

Evidencia de Revisión
Como evidencia de revisión, este papel de trabajo debe ser firmado por quien lo realizó y revisó.

Nombre		Fecha (dd/mm/aaaa):	Firma
Elaboró:			
Revisó:			

1. Definición del proceso que abarca el alcance de la revisión

Describen un conjunto organizado de prácticas y actividades para alcanzar ciertos objetivos y producir un conjunto de resultados que soporten las metas generales relacionadas con TI.

EDM01 Asegurar la configuración y el mantenimiento del marco de gobierno

Analiza y articula los requerimientos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadores, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa.

2. Definir los habilitadores relacionados

El alcance de este compromiso de aseguramiento es un proceso, sin embargo, según el modelo de habilitación COBIT 5, todos los habilitadores relacionados deberán considerarse también para su inclusión en el alcance. Defina los habilitadores que se incluirán en el alcance de su revisión:

Habilitador	Definición	Alcance
Principios, políticas y marcos	Son el vehículo para traducir el comportamiento deseado en guías prácticas para la gestión del día a día.	
Estructuras organizacionales	Son las entidades de toma de decisiones clave en una organización.	
Cultura, ética y comportamiento	De los individuos y de la empresa son muy a menudo subestimados como factor de éxito en las actividades de gobierno y gestión.	
Información	La información es necesaria para mantener la organización funcionando y bien gobernada, pero a nivel operativo, la información es muy a menudo el producto clave de la empresa en sí misma.	
Personas, habilidades y competencias	Están relacionadas con las personas y son necesarias para poder completar de manera satisfactoria todas las actividades y para la correcta toma de decisiones y de acciones correctivas.	
Servicios, Infraestructura y Aplicaciones	Incluyen la infraestructura, tecnología y aplicaciones que proporcionan a la empresa, servicios y tecnologías de procesamiento de la información.	

4.7 Entendimiento del proceso de gobierno de TI

El objetivo de este papel de trabajo es obtener la comprensión del proceso de gobierno de las tecnologías de información, que permita establecer los criterios de evaluación adecuados.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	**Cuestionario de Auditoría** **EDM01**			**Referencia:** ____ **Versión**: 01
Fecha aprobación:	**Nombre de la Empresa**			Páginas: 3
Objetivo: El objetivo de este cuestionario es obtener un entendimiento del nivel de ejecución de las actividades sugeridas por el proceso EDM01 de Cobit 5 y ISO/IEC 38500:2008 en el proceso de Gobierno de Tecnologías de Información. El cuestionario es de respuesta cerrada, bajos las opciones de "Si" o "No".				
Auditor:				
Criterios de auditoria:	Cobit 5, EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno			
Pregunta	**SI**	**NO**	**Procedimiento siguiente**	**Referencia**
EDM01.01 Evaluar el sistema de gobierno. Identificar y comprometerse continuamente con las partes interesadas de la empresa, documentar la comprensión de los requerimientos y realizar una estimación del actual y futuro diseño del Gobierno de Tecnologías de Información de la empresa.				
¿Analizan la Junta Directiva y el Comité de Estrategia cómo puede influir el entorno interno y externo del negocio en el diseño del Gobierno de las Tecnologías de Información?				
¿Se incluye como tema de agenda de Junta Directiva, el papel de TI en el negocio?				
¿Se realiza alguna evaluación de cómo se gestionan los requerimientos legales y contractuales mediante el Gobierno de las Tecnologías de Información?				
¿Se alinean las tecnologías de información con los intereses de las partes interesadas, objetivos, visión y dirección de la empresa?				
¿Se determinan las implicaciones de TI en el ambiente de control de la empresa?				
¿Se han definido los principios que guiarán el Gobierno de las Tecnologías de Información?				
¿Existe un modelo aprobado por la Junta Directiva para la toma de decisiones para tecnologías de información?				
¿Estan definidos formalmente los niveles y umbrales para la toma de decisiones de tecnologías de información?				
Principios de Gobierno de Tecnologías de Información El estándar ISO/IEC 38500 provee un marco de 6 principios básicos para que los directores lo utilicen cuando evalúen, dirijan y supervisen el uso de las TI en sus empresas. Seguir estos principios ayudará a los directores a balancear riesgos y propiciar oportunidades derivadas del uso de las TI.				

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	**Cuestionario de Auditoría EDM01**			**Referencia: ____ Versión:** 01
Fecha aprobación:	**Nombre de la Empresa**			Páginas: 3
Objetivo: El objetivo de este cuestionario es obtener un entendimiento del nivel de ejecución de las actividades sugeridas por el proceso EDM01 de Cobit 5 y ISO/IEC 38500:2008 en el proceso de Gobierno de Tecnologías de Información. El cuestionario es de respuesta cerrada, bajos las opciones de "Si" o "No".				
Auditor:				
Criterios de auditoria:	Cobit 5, EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno			
Pregunta	**SI**	**NO**	**Procedimiento siguiente**	**Referencia**
Principio 1: Responsabilidad: ¿Están claramente definidas las estructuras de la organización de gobierno, así como funciones y responsabilidades correctamente asignadas por la dirección, que proporcionen claridad en cuanto a la autoría y la rendición de cuentas por las tareas y decisiones importantes? Esto debería incluir las relaciones con proveedores críticos de servicios de TI.				
Principio 2: Estrategia: ¿Existe una planificación estratégica de tecnologías de información que se alinea con los objetivos estratégicos del negocio?				
Principio 3: Adquisión ¿Al analizar la viabilidad de adquisiones de tecnologías, se analizan integralmente su impacto en el negocio, la arquitectura, la capacitación del recurso humano, procesos del negocio, etc?				
Principio 4: Desempeño: ¿Se realiza la aprobación de los objetivos de desempeño de TI por las partes interesadas, y se realiza rendición de cuentas sobre el cumplimiento de los mismos?				
Principio 5: Conformidad: ¿Se toma en cuenta el cumplimiento de los requisitos legales y regulatorios como parte de la planificación estratégica o se solventan los temas de forma reactiva al gestionar las tecnologías de información?				
Principio 6: El comportamiento humano: ¿Se gestionan los cambios de tecnología evaluando el impacto en el comportamiento y cultura de la empresa, entrenando y mejorando las habilidades del personal y socios del negocio?				
EDM01.02 Orientar el sistema de gobierno.				
Informar a los líderes y obtener su apoyo, su aceptación y su compromiso. Guiar las estructuras, procesos y prácticas para el Gobierno de TI en línea con los principios, modelos para la toma de decisiones y niveles de autoridad diseñados para el gobierno. Definir la información necesaria para una toma de decisiones informadas.				
¿Se han realizado comunicaciones a las partes interesadas de los principios de Gobierno de las Tecnologías de Información?				
¿Estan establecidas las estructuras, procesos y prácticas del Gobierno de las Tecnologías de Información en línea con los principios de diseño acordados?				

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	**Cuestionario de Auditoría EDM01**			**Referencia: ____ Versión:** 01
Fecha aprobación:	**Nombre de la Empresa**			Páginas: 3
Objetivo: El objetivo de este cuestionario es obtener un entendimiento del nivel de ejecución de las actividades sugeridas por el proceso EDM01 de Cobit 5 y ISO/IEC 38500:2008 en el proceso de Gobierno de Tecnologías de Información. El cuestionario es de respuesta cerrada, bajos las opciones de "Si" o "No".				
Auditor:				
Criterios de auditoria:	Cobit 5, EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno			
Pregunta	**SI**	**NO**	**Procedimiento siguiente**	**Referencia**
¿Están claramente asignadas las responsabilidades en relación con la aplicación de los principios de gobierno, el cumplimiento de los modelos de toma de decisión y los umbrales establecidos?				
¿Estan definidos los canales de comunicación para los órganos encargados de la supervisión y toma de decisiones?				
¿Se concientiza al personal sobre directrices de comportamiento ético y profesional y se les comunican las consecuencias del no cumplimiento de las mismas?				
¿Existen sistemas de compensación que promuevan la cultura deseable en la organización?				
EDM01.03 Supervisar el sistema de gobierno.				
Supervisar la ejecución y la efectividad del Gobierno de TI de la empresa. Analizar si el sistema de gobierno y los mecanismos implementados (incluyendo estructuras, principios y procesos) están operando de forma efectiva y proporcionan una supervisión apropiada de TI.				
¿Se realizan evaluaciones de las partes interesadas en las que se ha delegado la responsabilidad y autoridad para el Gobierno de las Tecnologías de la empresa?				
¿Se evalúa periodicamente si las estructuras, principios, procesos acordados para el Gobierno de TI están establecidos y operan efectivamente?				
¿Se evalúa si el Gobierno de las Tecnologías esta funcionando de forma efectiva?				
En caso de identificar desviaciones en la evaluación del Gobierno de las Tecnologías ¿Se toman acciones para rectificar?				
¿Se supervisa que las tecnologías de información gestionan las regulaciones vigentes, politicas internas, estándares y directrices?				
¿Existen órganos o procesos rutinarios que se encarguen garantizar que las TI cumplen con las obligaciones regulatorias, estándares y directrices?				

4.8 Entendimiento habilitador principios, políticas y marcos

El objetivo de este papel de trabajo es obtener la comprensión del habilitador Principios, Políticas y Marcos de referencia para el gobierno de las tecnologías de información.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	**Cuestionario de Auditoría** **Habilitador principios, políticas y marcos**	Referencia: _____ Versión: 01
Fecha aprobación:	**Nombre de la Empresa**	Páginas: 2

Objetivo: El objetivo de este cuestionario es obtener un entendimiento del nivel del nivel de ejecución del habilitador de principios, políticas y marcos de referencia que según lo define COBIT 5, abarca los mecanismos de comunicación disponibles para trasmitir la dirección e instrucciones de los cuerpos de gobierno y de dirección.

Auditor:

Criterios de auditoria: COBIT® 5, Apéndice G - Descripción detallada de los catalizadores de COBIT 5

Pregunta	SI	NO	Comentarios	Procedimiento siguiente	Referencia
Partes Interesadas En los principios y políticas, las partes interesadas pueden ser internas o externas a la empresa. Éstas incluyen el Consejo y el comité ejecutivo de dirección, directores de cumplimiento, gerentes de riesgos, auditores internos y externos, proveedores del servicio, clientes y agencias reguladoras. Sus intereses están divididos: Algunas partes interesadas definen y establecen las políticas mientras que las otras tienen que alinearse y cumplir con ellas.					
¿Están definidos los responsables de definir y establecer las políticas relacionadas con tecnologías de información?					
Si la respuesta anterior fue positiva indique el nombre de las personas responsables:					
Indique el nombre de la persona autorizada para aprobar las políticas y autorizar cambios en éstas.					
¿Existe un repositorio con las políticas vigentes y autorizadas formalmente?					
¿Se comunican periódicamente las políticas vigentes?					
¿Se evalúa el cumplimiento de las políticas vigentes?					
Metas Cada habilitador cuenta con una serie de metas. Los habilitadores proporcionan valor mediante la consecución de dichas metas. Las metas se pueden definir en términos de: Resultados esperados del habilitador y aplicación u operativa del propio habilitador					
¿Existen principios bases definidos para la gestión de la asociación?					
Si la respuesta anterior fue positiva, indíquelos:					
¿Existen políticas definidas formalmente?					
¿Está definido el propósito en cada política?					
¿Existen mecanismos que proporcionen un acceso fácil a las políticas a todas las partes interesadas?					
¿Saben las partes interesadas dónde encontrar las políticas?					
¿Se han definido marcos de referencia para la gestión de las políticas de tecnologías de información?					
Si la respuesta anterior fue positiva, indiquelos:					
Ciclo de vida Cada catalizador tiene un ciclo de vida, desde su comienzo pasando por su operación/vida útil hasta su retirada. Las fases del ciclo de vida consisten en: – Planificación (que incluye el desarrollo y selección de conceptos) – Diseño – Construcción/adquisición/creación/implementación – Uso/operación – Evaluación/supervisión – Actualización/retirada. Las políticas tienen un ciclo de vida que ha de apoyar la consecución de las metas definidas.					
¿Existe un proceso periódico de actualización de los principios, políticas y marcos de referencia?					
¿Existen mecanismos para que las partes interesadas estén al tanto de cambios en principios, políticas, marcos de referencia?					
¿Se ponen a disposición de las partes interesadas y se comunican los cambios autorizados?					
¿Existe un procedimiento para gestionar las versiones de las políticas?					
Buenas prácticas					

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	**Cuestionario de Auditoría Habilitador principios, políticas y marcos**	Referencia: _____ Versión: 01
Fecha aprobación:	**Nombre de la Empresa**	Páginas: 2

Objetivo: El objetivo de este cuestionario es obtener un entendimiento del nivel del nivel de ejecución del habilitador de principios, políticas y marcos de referencia que según lo define COBIT 5, abarca los mecanismos de comunicación disponibles para trasmitir la dirección e instrucciones de los cuerpos de gobierno y de dirección.

Auditor:

Criterios de auditoria: COBIT® 5, Apéndice G - Descripción detallada de los catalizadores de COBIT 5

Pregunta	SI	NO	Comentarios	Procedimiento siguiente	Referencia
Las buenas prácticas proporcionan ejemplos o sugerencias respecto a la mejor manera de implementar el habilitador y qué productos de trabajo o entradas y salidas se requieren. Las buenas prácticas requieren que las políticas formen parte del marco de gobierno y de gestión general, proporcionando una estructura (jerárquica) a la que deberían ceñirse todas las políticas y actuando de enlace con los principios subyacentes.					
¿Existe un marco de gestión de políticas?					
¿Está establecido en este marco su alcance, las consecuencias de cumplir las políticas, la gestión de excepciones y cómo se evaluará el cumplimiento de las políticas?					
¿Se evalúan las políticas con el apetito de riesgo de la asociación?					
¿Está establecido en este marco la periodicidad para la revisión de las políticas?					

4.9 Entendimiento habilitador Estructuras Organizativas

El objetivo de este papel de trabajo es obtener la comprensión del habilitador Estructuras Organizativas para el gobierno de las tecnologías de información.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	**Cuestionario de Auditoría Habilitador Estructuras Organizativas**	Referencia: _____ Versión: 01
Fecha aprobación:	**Nombre de la Empresa**	Páginas: 2

Objetivo: El objetivo de este cuestionario es obtener un entendimiento del nivel del nivel de ejecución del habilitador estructuras organizativas identificando as entidades de toma de decisiones clave en la asociación.

Auditor:

Criterios de auditoria: COBIT® 5, Apéndice G - Descripción detallada de los catalizadores de COBIT 5

Pregunta	SI	NO	Comentarios	Procedimiento siguiente	Referencia
Partes Interesadas Las partes interesadas en las estructuras organizativas pueden ser internas y externas a la empresa e incluyen a: los miembros individuales de la estructura, otras estructuras, entidades organizativas, clientes, proveedores y reguladores. Sus roles varían e incluyen la toma de decisiones, influenciar y asesorar. Las participaciones de cada una de las partes interesadas también varían.					
¿Está definido el rol de la Junta Directiva en relación con las tecnologías de información?					
Indique qué tipo de decisiones toma la Junta Directiva en relación con las tecnologías de información.					
¿Está definido el rol del comité ejecutivo de estrategia en relación con las tecnologías de información?					
Indique qué tipo de decisiones toma el comité ejecutivo de estrategia en relación con las tecnologías de información.					
¿Está definido el rol de la Gerente de Operaciones en relación con las tecnologías de información?					
Indique qué tipo de decisiones toma el Gerente de Operaciones en relación con las tecnologías de información.					
¿Está definido el rol del Encargado de tecnologías de información en relación con las tecnologías de información?					
Indique qué tipo de decisiones toma el Encargado de tecnologías de información en relación con las tecnologías de información.					
Metas Cada habilitador cuenta con una serie de metas. Los habilitadores proporcionan valor mediante la consecución de dichas metas. Las metas se pueden definir en términos de: Resultados esperados del habilitador y aplicación u operativa del propio habilitador					
¿Están claramente establecidos y son comunicados los roles de la estructura organizativa?					
¿Es realizada la toma de decisiones bajo los roles establecidos?					
Ciclo de vida Cada habilitador tiene un ciclo de vida, desde su comienzo pasando por su operación/vida útil hasta su retirada. Las fases del ciclo de vida consisten en: – Planificación (que incluye el desarrollo y selección de conceptos) – Diseño – Construcción/adquisición/creación/implementación – Uso/operación – Evaluación/supervisión – Actualización/retirada.					
¿Se evalúa periódicamente la estructura organizativa?					
Indique quién realiza esta evaluación y aprueba los cambios.					
¿Existe un proposito definido que justifique la estructura organizativa actual?					

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	**Cuestionario de Auditoría** **Habilitador Estructuras Organizativas**	Referencia: _____ Versión: 01
Fecha aprobación:	**Nombre de la Empresa**	Páginas: 2

Objetivo: El objetivo de este cuestionario es obtener un entendimiento del nivel del nivel de ejecución del habilitador estructuras organizativas identificando as entidades de toma de decisiones clave en la asociación.

Auditor:

Criterios de auditoria: COBIT® 5, Apéndice G - Descripción detallada de los catalizadores de COBIT 5

Pregunta	SI	NO	Comentarios	Procedimiento siguiente	Referencia
Buenas prácticas Las buenas prácticas proporcionan ejemplos o sugerencias respecto a la mejor manera de implementar el habilitador y qué productos de trabajo o entradas y salidas se requieren.					
¿Existen principios operativos definidos para cada componente de la estructura que incluyan las modalidades prácticas respecto a cómo la estructura operará, tales como frecuencia de reuniones, documentación, reglas de mantenimiento, perfiles de puesto?					
¿Están definidos formalmente los miembros de Junta Directiva y Comité de Estrategia?					
¿Están claramente definidos los límites en la toma de decisiones para cada estructura en relación con tecnologías de información?					

4.10 Entendimiento habilitador Personas, Habilidades y Competencias

El objetivo de este papel de trabajo es obtener la comprensión del habilitador Personas, Habilidades y Competencias para el gobierno de las tecnologías de información.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	**Cuestionario de Auditoría Habilitador personas, habilidades y competencias**	Referencia: _____ Versión: 01
Fecha aprobación:	**Nombre de la Empresa**	Páginas: 2

Objetivo: El objetivo de este cuestionario es obtener un entendimiento del nivel del nivel de ejecución del habilitador personas, habilidades y competencias, mismos que son necesarios para poder completar de manera satisfactoria todas las actividades y para la correcta toma de decisiones y de acciones correctivas.

Auditor:

Criterios de auditoria: COBIT® 5, Apéndice G - Descripción detallada de los catalizadores de COBIT 5

Pregunta	SI	NO	Comentarios	Procedimiento siguiente	Referencia
Partes Interesadas Las capacidades y competencias de las partes interesadas son internas y externas a la empresa. Diferentes interesados asumen diferentes roles— directivos empresariales, gerentes de proyecto, socios, competidores, formadores, reclutadores, desarrolladores, técnicos especialistas en IT, etc. —y cada papel requiere un conjunto de habilidades diferentes.					
¿Considera que la Junta Directiva tiene los conocimientos necesarios en tecnologías de información para guiar la gobernanza de las TI?					
Indique cuáles miembros de Junta Directiva considera que proporcionan mayor apoyo en este tema:					
¿Conoce la Junta Directiva de marcos de gobernanza de las tecnologías de información?					
Indique cuáles marcos:					
¿Considera que usted tiene los conocimientos necesarios de TI para la gestión de su rol en la toma de decisiones de TI?					
Indique el perfil de su puesto:					
¿Considera que el Encargado de TI tiene los conocimientos necesarios para la gestión de su rol?					
Indique el perfil del puesto del Encargo de TI					
Metas Cada habilitador cuenta con una serie de metas. Los habilitadores proporcionan valor mediante la consecución de dichas metas. Las metas se pueden definir en términos de: Resultados esperados del habilitador y aplicación u operativa del propio habilitador					
¿Se han realizado en el último año actividades de capacitación a las partes interesadas acerca de marcos de tecnologías de información?					
¿Se han realizado actividades de capacitación en TI a las partes interesadas cuyo rol corresponde a tomadores de decisión?					
Indique los años de experiencia del personal a cargo de las TI:					
¿Considera que tiene el personal suficiente para la gestión de las TI					
¿Tiene el personal encargado de las TI conocimientos verificados mediante certificados profesionales, títulos, etc.?					
Ciclo de vida Cada habilitador tiene un ciclo de vida, desde su comienzo pasando por su operación/vida útil hasta su retirada. Las fases del ciclo de vida consisten en: – Planificación (que incluye el desarrollo y selección de conceptos) – Diseño – Construcción/adquisición/creación/implementación – Uso/operación – Evaluación/supervisión – Actualización/retirada.					
¿Se han evaluado las capacidades del personal de TI en relación con las nuevas exigencias de TI en la organización?					
Indique cuándo se realizó la última evaluación					
¿Existe un plan de desarrollo formal para las competencias en TI?					

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	**Cuestionario de Auditoría Habilitador personas, habilidades y competencias**				Referencia: _____ Versión: 01
Fecha aprobación:	**Nombre de la Empresa**				Páginas: 2
Objetivo: El objetivo de este cuestionario es obtener un entendimiento del nivel del nivel de ejecución del habilitador personas, habilidades y competencias, mismos que son necesarios para poder completar de manera satisfactoria todas las actividades y para la correcta toma de decisiones y de acciones correctivas.					
Auditor:					
Criterios de auditoria:	COBIT® 5, Apéndice G - Descripción detallada de los catalizadores de COBIT 5				
Pregunta	**SI**	**NO**	**Comentarios**	**Procedimiento siguiente**	**Referencia**
¿Se debe su estrategia de contratación de proveedores TI externos a insuficientes capacidades y recursos internos para proveer servicios de TI?					
¿Existe presupuesto destinado a la capacitación en TI para las partes interesadas?					
Buenas prácticas					
Las buenas prácticas proporcionan ejemplos o sugerencias respecto a la mejor manera de implementar el habilitador y qué productos de trabajo o entradas y salidas se requieren.					
¿Están definidas las habilidades requeridas en cada puesto u órgano en relación con las TI?					
¿Se identifica la brecha existente en esas habilidades y las requeridas?					
¿Se incluyen las habilidades a desarrollar en el plan formal de capacitación?					
¿Se tiene algún marco de referencia como guía de las habilidades y competencias requeridas?					

4.11 Entendimiento habilitador Servicios, Infraestructura y Aplicaciones

El objetivo de este papel de trabajo es obtener la comprensión del habilitador Servicios, Infraestructura y Aplicaciones para el gobierno de las tecnologías de información.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	**Cuestionario de Auditoría Habilitador Servicios, Infraestructura y Aplicaciones**	Referencia: _____ Versión: 01
Fecha aprobación:	**Nombre de la empresa**	Páginas: 2

Objetivo: El objetivo de este cuestionario es obtener un entendimiento del nivel de ejecución del habilitador incluyen la infraestructura, tecnología y aplicaciones que proporcionan a la empresa, servicios y tecnologías de procesamiento de la información.

Auditor:

Criterios de auditoria: COBIT® 5, Apéndice G - Descripción detallada de los catalizadores de COBIT 5

Pregunta	SI	NO	Comentario	Procedimiento siguiente	Referencia
Partes Interesadas Las partes interesadas de las capacidades de servicio (el concepto combinado de servicios, infraestructura y aplicaciones) pueden ser internas y externas. Los servicios pueden ser entregados por las partes internas o externas					
¿Se tienen identificados los usuarios internos y externos de los servicios de TI (servicios, infraestructura y aplicaciones) a nivel de proveedores de servicio y receptores de los servicios?					
¿Se tiene identificado el rol de cada parte interesada en los servicios de TI?					
Indique los responsables de una entrega adecuada de servicios de TI a las partes interesadas.					
¿Existen proveedores de servicios externos?					
¿Existen receptores de servicios externos?					
¿Se tiene un documento o diagrama identificando todos los servicios, infraestructura y aplicaciones y su uso actual?					
Metas Cada habilitador cuenta con una serie de metas. Los habilitadores proporcionan valor mediante la consecución de dichas metas. Las metas se pueden definir en términos de: Resultados esperados del habilitador y aplicación u operativa del propio habilitador					
¿Se tienen definidos niveles de servicio deseado para las aplicaciones y servicios de TI internos?					
¿Están documentados estos niveles de servicio definidos?					
¿Existen acuerdos de nivel de servicio (SLA, por sus siglas en inglés) con los proveedores de TI externos?					
Indique quién es el responsable de definir los niveles de servicio de TI.					
¿Se han presentado incidentes de servicios en el último año?					
¿Se documentan los incidentes en servicios de tecnologías?					
Ciclo de vida Cada habilitador tiene un ciclo de vida, desde su comienzo pasando por su operación/vida útil hasta su retirada. Las fases del ciclo de vida consisten en: – Planificación (que incluye el desarrollo y selección de conceptos) – Diseño – Construcción/adquisición/creación/implementación – Uso/operación – Evaluación/supervisión – Actualización/retirada.					
¿Esta definida la arquitectura de TI?					
¿Existe una arquitectura de TI de referencia o modelo que permita identificar brechas y realizar mejoras en aras de disminuir la brecha existente con la arquitectura actual?					
¿Es evaluada periódicamente la arquitectura de TI por los órganos de dirección?					

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	**Cuestionario de Auditoría Habilitador Servicios, Infraestructura y Aplicaciones**	Referencia: _____ Versión: 01
Fecha aprobación:	**Nombre de la empresa**	Páginas: 2

Objetivo: El objetivo de este cuestionario es obtener un entendimiento del nivel de ejecución del habilitador incluyen la infraestructura, tecnología y aplicaciones que proporcionan a la empresa, servicios y tecnologías de procesamiento de la información.

Auditor:

Criterios de auditoria: COBIT® 5, Apéndice G - Descripción detallada de los catalizadores de COBIT 5

Pregunta	SI	NO	Comentario	Procedimiento siguiente	Referencia
¿Se alinean el desarrollo de aplicaciones y cambios en TI con la arquitectura deseada?					
Buenas prácticas					
Las buenas prácticas proporcionan ejemplos o sugerencias respecto a la mejor manera de implementar el habilitador y qué productos de trabajo o entradas y salidas se requieren.					
¿Estan definidos los principios de arquitectura a seguir? (Algunos principios: **Comprar frente a construir**—Las soluciones deberían ser adquiridas a menos que exista una razón para aprobar su desarrollo interno. **Simplicidad**—La arquitectura de la empresa debería ser diseñada y mantenida para ser tan simple como sea posible sin dejar de cumplir con los requisitos de la empresa. **Agilidad**—La arquitectura de la empresa debería incorporar agilidad para satisfacer las cambiantes necesidades de negocio de una manera eficaz y eficiente.)					
¿Se utiliza algún marco de referencia de arquitectura y de servicios?					
¿Existe un repositorio de la documentación autorizada y vigente relacionada con la arquitectura de TI?					

CAPÍTULO 5- ANÁLISIS DE RESULTADOS

Una vez aplicadas las plantillas incluidas en el capítulo cuatro se procedió a realizar el análisis de la información recopilada, con el objetivo de determinar los hallazgos a incluir en el informe preliminar de auditoría. Cabe mencionar que los hallazgos de auditoría están sustentados en evidencia suficiente, competente y pertinente, obtenida por los medios legales y técnicos aplicables.

El análisis de la información fue realizado en diferentes etapas conforme se aplicaron las diferentes herramientas y se resumen de la siguiente forma:

- ➜ El entendimiento de la entidad y su entorno: Mediante su análisis fue posible definir las prioridades estratégicas identificadas en objetivos concretos para el proceso de auditoría, además determinar los principales habilitadores a evaluar.
- ➜ Entendimiento del proceso de gobierno de las TI: El objetivo de este papel de trabajo era obtener la comprensión del proceso de gobierno de las tecnologías de información, que permitiera establecer los criterios de evaluación adecuados, para lo cual se dividió este entendimiento en cuatro secciones, compuestas por los tres subprocesos del proceso “EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno” y una sección que contenía preguntas relacionadas con los principios establecidos en el estándar ISO/IEC 38500. En general, de las respuestas obtenidas, se evidencia una brecha importante en las estructuras de gobierno de las TI, principalmente porque se identifica que no están definidos los principios que establecen el rol y sientan las bases que guían la toma de decisiones de las TI en la Asociación; la toma de decisiones de TI se realiza bajo el criterio de la Administración y se basa en reaccionar a las necesidades del mercado y las necesidades internas, con poca participación de los órganos de dirección; tampoco se realizan análisis de los factores del entorno interno y externo (obligaciones legales, contractuales y regulatorias)

y tendencias en el entorno del negocio, por parte de los órganos de dirección, que puedan influir en el diseño del gobierno de las TI; no existe un plan estratégico de TI, ni un proceso de evaluación o supervisión que permita medir que el enfoque de gestión de las TI está direccionado a apoyar el cumplimiento de los objetivos del negocio. La administración considera que las TI están alineadas con la estrategia del negocio, pero no existen mecanismos de medición que permitan verificar esta aseveración y tampoco la intervención de los órganos de dirección en estos temas que permita verificar la efectividad del proceso. Estas situaciones se incorporan en el informe de comunicación de resultados, con sus respectivas recomendaciones.

- ➜ Entendimiento de los habilitadores definidos en el alcance: El objetivo de la recopilación de esta información era determinar cómo los habilitadores influyen positiva o negativamente en el gobierno de las TI. Se analizaron las respuestas para cada habilitador identificando deficiencias en estas estructuras que están afectando el gobierno de las TI, este análisis se realiza basado en las dimensiones comunes que establece COBIT 5 para cada habilitador incluido en el alcance. El habilitador Estructuras organizativas permitió identificar que no están definidos los roles de los órganos de dirección en relación con el gobierno de las TI, el no involucrar a la Junta Directiva u órganos estratégicos en el gobierno de las TI limita su visión estratégica y su alineación con los objetivos, llevando a las TI a un proceso de gestión operativa y no como un pilar estratégico de la asociación. El análisis del habilitador Personas, habilidades y competencias permitió identificar que existe ausencia de capacitación y concientización de los órganos de dirección y gerencia en relación con temas de gobierno de las TI lo que limita al alcance y evolución que pueden tener en las TI en la Asociación. El análisis del habilitador Principios, políticas y marcos de referencia permitió identificar que no existen políticas de gobernanza, de gestión y de uso de recursos de TI. Aunque existen repositorios de políticas

de operación no se han desarrollado políticas de TI, por ende, no existe ningún marco de gestión de estas políticas.

El informe preliminar de auditoría se elaboró en un lenguaje sencillo, objetivo, conciso, claro, completo, exacto e imparcial, basado en hechos y respaldado con evidencia suficiente, competente y pertinente.

Cada hallazgo está compuesto por información que permite identificar la situación actual encontrada, la causa que originó la desviación, el efecto que podría tener si se materializa la situación detectada y finalizando con el criterio de la norma o marco de referencia aplicable donde se indica cómo debe ser.

Finalmente, se emitieron las recomendaciones pertinentes a las autoridades respectivas de la Asociación, a fin de que se tomen las acciones necesarias con el fin de solucionar el hallazgo detectado. Las recomendaciones contemplaron al menos lo siguiente: a) Generar valor a la entidad b) Atacar las causas del problema o condición identificada, c) Dirigidas al nivel responsable de solventar la deficiencia y d) Ser claras, específicas, convincentes y relevantes.

CAPÍTULO 6- CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones del estudio aplicado y sus recomendaciones

A continuación, se describen las principales conclusiones y recomendaciones del estudio realizado, estas se realizan de forma general manteniendo la confidencialidad de la organización.

6.1.1 Conclusiones

En concordancia con el objetivo y el alcance del presente estudio se concluye producto del estudio aplicado, que la organización no ha diseñado ni mantiene funcionando estructuras de gobierno de las tecnologías de información, determinando una brecha significativa entre estas estructuras y las mejores prácticas.

Lo anterior sucede debido a la inexistencia de principios relacionados con el gobierno de las TI, la ausencia de una evaluación de la alineación de las TI con la estrategia de la Asociación, la inexistencia de un plan estratégico de TI, la no definición formal de los roles de las estructuras organizativas en relación con este proceso, ausencia de capacitación y concientización de los órganos de dirección y gerencia en relación con temas de gobierno de las TI y la inexistencia de marcos y políticas formales de gobernanza de TI.

Las situaciones identificadas pueden estar limitando a la Asociación a garantizar que las decisiones relacionadas con TI se han tomado en línea con las estrategias y objetivos, debido a la inexistencia de un enfoque consistente, integrado y alineado con el gobierno de la Asociación.

6.1.2 Recomendaciones

A la Junta Directiva

Establecer los principios básicos para evaluar, dirigir y supervisar el uso de las TI en la Asociación. La adopción de estándares internacionales como las normas ISO, podría constituir un punto de partida, en específico la norma ISO/IEC 38500 proporciona un marco que puede ser utilizado por la Asociación como mejor práctica para el establecimiento de estos principios.

Solicitarle a la administración el desarrollo de un plan estratégico de Ti que integre la visión estratégica del negocio con la visión estratégica de las TI y proporcione orientación a TI para la ejecución de proyectos estratégicos que soporten a la asociación en cumplir su visión y misión, este plan debe proporcionar un camino a seguir para lograr las estructuras de TI deseadas en el largo plazo, debe ser aprobado por la Junta Directiva y sometido a seguimiento con periodicidades establecidas por este órgano.

Definir su rol en relación con el gobierno de las TI y definir las estructuras organizacionales, comités, roles y procesos formales de gobierno. Es de suma importancia que la Junta Directiva active su involucramiento en los temas relacionados con las TI y aclare el proceso de toma de decisión, definiendo qué decisiones podrán tomar los diferentes órganos en relación con la administración y el uso de las TI y cómo se tomarán y se monitorearán esas decisiones.

Conformar un Comité de TI, que constituya un órgano asesor y de coordinación en temas estratégicos relacionados con el uso de las TI, fortaleciendo su conformación con personal que reúna competencias fuertes en lo relacionado con la TI y el entendimiento de la estrategia de la Asociación.

Utilizar asesores externos en temas de TI que apoyen a la Junta Directiva en la conformación y toma de decisión de todas las estructuras tanto para la gobernanza como la gestión de las TI.

A la Gerencia de Operaciones

Realizar un proceso de concientización a nivel de Junta Directiva sobre la necesidad de implantar mecanismos de gobernanza, evaluar mejores prácticas implementadas en entidades similares.

Desarrollar un plan de capacitación con asesoría de un experto tanto para los órganos de dirección como para la administración en relación con temas de gobernanza y gestión de TI.

Concientizar a los miembros de Junta Directiva sobre el papel de las tecnologías de información en la organización mediante expertos independientes y las ventajas que estructuras de gobernanza le pueden proporcionar a la asociación.

6.2 Conclusiones del proyecto realizado

A continuación, se describen las principales conclusiones del proyecto realizado:

Existen herramientas a disposición del auditor que permiten realizar una evaluación de esta naturaleza bajo una estructura basada en mejores prácticas. El uso de los recursos de ISACA y marcos como COBIT 5 le otorga profesionalismo al proyecto y además, facilita la planificación y ejecución.

El tamaño de la organización no representó una limitación al realizar la evaluación, aunque las estructuras de gobierno tenían un nivel de madurez muy bajo no fue por su tamaño, sino principalmente por la ausencia de concientización del tema.

Las herramientas desarrolladas son de fácil aplicación y comprensión y permiten obtener evidencia de una forma práctica de las estructuras de gobierno de TI.

El enfoque holístico que proporciona el uso de los habilitadores, según el marco COBIT 5, permite proporcionar un enfoque integral del tema, es sumamente relevante comprender su implementación.

El mayor desafío en el tema de gobernanza es la concientización y capacitación sobre su importancia y los beneficios que trae a las organizaciones, una inversión de recurso en este aspecto puede cambiar el giro en el abordaje de este tema de forma significativa.

6.3 Recomendaciones generales

A continuación, se indican las principales recomendaciones a nivel general una vez realizado el proyecto:

Es importante que las organizaciones adopten marcos de referencia que sean utilizados como mejores prácticas para la mejora de temas como el desarrollado en el presente trabajo, entre estos se encuentran COBIT 5 y la norma ISO/IEC 38500; y que sus directores y ejecutivos conozcan a fondo las ventajas de su implementación.

Que las organizaciones se sometan a procesos de auditoría que les permitan identificar oportunidades de mejora y realizar seguimiento a la implementación de recomendaciones de forma que un órgano independiente pueda proporcionar una seguridad razonable de que los procesos se están ejecutando bajo los principios, políticas y marcos definidos.

Los profesionales de auditoría de TI deben tener conocimiento adecuado tanto de la organización como de las mejores prácticas que les permitan ejecutar un proceso de auditoría de esta naturaleza con ética, profesionalismo y con un enfoque de generar valor agregado a la organización. La actualización constante, la obtención de certificaciones son parte de las herramientas que robustecen la profesión.

BIBLIOGRAFÍA

Asociación Colombiana de Ingenieros en Sistemas. (2015). *Evolución del Gobierno Digital*. Revista Sistemas, 136(Jul-Set): Recuperado de: http://52.1.175.72/portal/sites/all/themes/argo/revista/Sistemas136.pdf

Ballester, M. (2010*). JOnline: Gobierno de las TIC ISO/IEC 38500*. The ISACA Journal, 1(1): Recuperado de: https://www.isaca.org/Journal/archives/2010/Volume-1/Pages/Gobierno-de-las-TIC-ISO-IEC-385001.aspx?utm_referrer=

Barrantes Echeverría, R. (1999). *Investigación. Un camino al conocimiento: Un Enfoque Cuantitativo y Cualitativo.* San José, Costa Rica: EUNED.

CONASSIF. (2017). *Reglamento General de Gestión de la Tecnología de Información*. La Gaceta de la República de Costa Rica N°71, 17 de abril del 2017. Recuperado de: https://www.sugef.fi.cr/normativa/normativa_vigente/documentos/SUGEF%2014-17%20(v2_%2017abr2017).pdf

Contraloría General de la República. (2014). *Normas Generales de Auditoría para el Sector Público:* Recuperado de: http://ocu.ucr.ac.cr/images/ArchivosOCU/Normativa/NormativaExterna/NormasGeneralesAuditoriaSectorPublico.pdf

Contraloría General de la República. (2007). *Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE)*. Recuperado de: http://ocu.ucr.ac.cr/images/ArchivosOCU/CapacitacionRIDS/N-2-2007-CO-DFOENormasGestionControlTI-CGR.pdf

Contraloría General de la República. (2009). *Reglamento sobre la Gestión de la Tecnología de la Información*. La Gaceta de la República de Costa Rica N°50, 12 de marzo del 2009. Recuperado de:

https://webcache.googleusercontent.com/search?q=cache:C2q5XQS_8S8J:https://www.sugef.fi.cr/normativa/normativa-vigente/documentos/SUGEF%252014-09.docx+&cd=2&hl=es-419&ct=clnk&gl=cr&client=safari

ISACA. (2012). *Contenidos de la Guía de Referencia de Procesos de COBIT 5*. En: COBIT 5: Procesos Catalizadores. Madrid: ISACA FRAMEWORK

ISACA. (2014). *Evaluate, Direct and Monitor: EDM0 Ensure Governance Famework Setting and Maintenance Audit/Assurance Program*. Bélgica: ISACA FRAMEWORK

ISACA. (2012). *Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* Madrid: ISACA FRAMEWORK